UOT:658

KART İŞLƏRİNDƏ BİRLƏŞMƏLƏRİN BİLDİRİLMƏSİ ÜZRƏ MƏLUMAT MƏDƏNÇİLİYİ TEXNİKASININ TƏTBİQİ

N. F. ƏLİYEV
Bakı Mühəndislik Universiteti

FRAUD termini təyin etmək üçün fərqli bir təsəvvür və bir neçə sahəyə malik olmasına baxmayaraq, fırıldaqçılıq səbəbindən başlıca uğursuzluq onlayn alış, poçt əməliyyatları, telefon əməliyyatları və s. Kimi "Kart yoxdur" əməliyyatı ilə bağlıdır. Kartdan dolandırıcılıq itkiləri milyardlarla dollar və yüksəlişdə. Scammers həmişə fırıldaqçılıq etmək üçün yeni yollar tapır və onlar sistem ətrafında necə olacağını bilirlər. Çox hallarda, fırıldaqçılıq anlaşılıb, fırıldaqçılıq artıq zəmanət verildikdən sonra baş verir. Buna görə də, kredit kartı fırıldaqçılığının aşkarlanması üsulları daimi yenilik tələb edir və bütün maliyyə institutları bu cür ssenarinin qarşısını almaq üçün bəzi saxtakar aşkarlama üsulları və ya üsulları olmalıdır. Data Mining əsasən bir nümunəni aşkarlamaq, emissiya və ya anomaliyaları aşkar etmək üçün bir vasitədir. Müxtəlif növ fırıldaqçılıqların aşkar edilməsi üçün yaxşı işləyir. Bu yazı, məlumatların tədqiqi əsasında saxta şəbəkənin dəstəklənməsi üçün vektor maşınları, K-ən yaxın qonşu, süni immun sistemi, peer qrupu analizi və s. Kimi bir sıra üsulları təhlil edir. Biz də tətbiq oluna bilən yeni bir texnika üçün təkliflər təqdim edirik və mövcud texnologiyaların mahiyyətini başa düşəcək və bir hissəsini birbaşa dolandırıcılıq aşkarlama vasitəsi ilə təmin edə bilər.

Açar sözlər: *Proqram mühəndisliyi, proqram təminatı inkişafı həyat dövrü, model-görünüş-müfəttiş arxitekturası*

Hal-hazırda, avtomatlaşdırılmış bir həyat üçün hər şeyi, hətta vacib və zəruri olmayan vəzifələri belə koordinasiya etmək gündəmə gəlmişdir. Texnologiyanın getdikcə yüksək inkişafı, ənənəvi və köhnə strukturların bütün sahələrində müasir qurğuların əvəzlənməsi ilə müşahidə olunur. Bu yüksəlişdən sonra bank sistemi müştərilərinə mümkün olan ən yüksək səmərəliliyi təmin etməyə çalışır. Texnoloji irəliləyişlər və inkişafları elektron bankçılıq sistemindən istifadə edilməyini də bu tendensiyanın davamı hesab etmək olar.

Son zamanlar, kredit kartı saxtakarlığının qarşısının alınması böyük bankların qarşısında duran əsas narahatlıq olmuşdur, çünki onlayn kredit kartı saxtakarlığı səviyyəsi ciddi şəkildə artmışdır. E-ticarətin kredit kartı saxtakarlığının aşkarlanması və cəzalandırılması kredit kartının tarixində risklərin idarə edilməsi mövzusunun çox vacib hissəsidir.

Buna görə, hazırkı tədqiqatın əsas məqsədi kredit kartlarında dolandırıcılığı şübhə altına alan məlumatların məbləğinin müəyyən edilməsi üçün yoxlanılmamış məlumat-mədən üsulunun təklif edilməsidir.

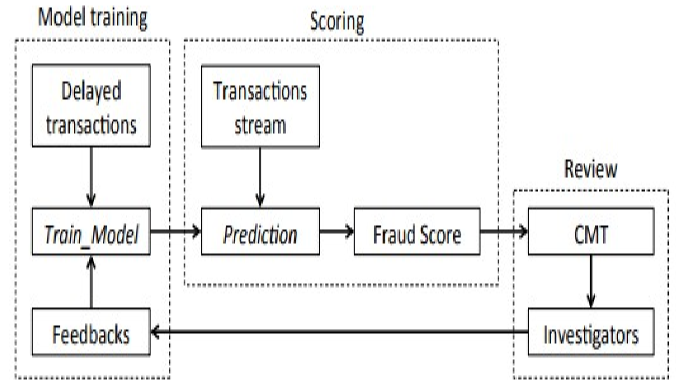
Bu məqalədə istifadə olunan tədqiqat metodikası 2017-ci ilin may ayından etibarən işləyən layihədən toplanan məlumatdır.

Dolandırıcı əməliyyatların aşkara çıxarılmasına məlumat mədənçiliyinin tətbiqi

Aşağıdakı şəkildən göründüyü kimi, istifadəçi ilk olaraq daha əvvəl olmuş əməliyyatlar vasitəsi ilə sistemi təlim etməlidir. Bu sistem 3 hissədən ibarətdir. İlk olaraq əməliyyatların özü sistemə daxil olunur. Daha sonra isə təlim modelsi sistemdə təyin olunur. Və nəhayət bu alt sistemə daxil olmuş əks

əlaqələr təlim metoduna qoşulur. İstifadəçi təyin olunan əməliyyata müvafiq model əlavə et düymə-sinə klikləyir. İşarələnmiş və işarələnməmiş əməliy-yatlar xüsusi siyahılara ilə doludur, bu da fırıl-daqçılıq aşkarlama kodunun mümkün variantları dərk etməyinə yardımçı olur. Fırıldaqçılıq aşkarlan-masında növbəti addım giriş göstəriş düyməsinə uyğun olub-olmadığını yoxlayır. Transaksiya girişi düzgün müəyyən edildikdə, istifadəçi onun doğrudan verilənlər bazasına əlavə etməyi seçə bilər. Bu vəziyyət insident və risk matrislərinin müvafiq sətirlərinin alınması və daxil olan əməliyyatın spesifikasiyalarının onlayn kodunun girişi ilə yenilənməsi ilə əldə edilir. Alternativ olaraq, istifadəçi birbaşa əməliyyatlar qrupunda audit edə bilər. Beləliklə, əməliyyatın daxil edilməsi yeniləmə üçün istifadə olunmur insidensiya və risk matrisi daimi olaraq. Bu qəbul edilən sətrin saxtakarlıq olduğu təqdirdə daxilolma və riski matrisləri gündəmə gətirməklə kodun icrasına bir az təsir edəcəkdir, çünki məlumat bazasında çıxışın sayını artırmaq nəhayət, satışların ən ümumi əməliyyatlara səbəb olacaqdır. Bu alətin bu saxta əməliyyatları aşkar etməsinə mane olur. Beləliklə, istifadəçi məlumat bazasına daxil olan əmliyyatı əlavə etməlidir. Və bundan sonra audit prosesindən çıxmış əməliyyatın saxta olmaması fikrini irəli sürmək olar.

Hesablama sistemi, məlumat bazasına aid əməliyyatları idarə etdiyi üçün, demək olar ki, modelin əsas bloku hesab olunur. Yuxarıda qeyd edildiyi kimi, təyin etmə əməliyyatları burada işlənir. İstək yalnız təyinat əməliyyatlarından ibarətdirsə, onda yalnız bu blok həyata keçirilir, yəni sorğu 1-ci planda göstərilən ümumi model bloku tərəfindən qəbul edilir və birbaşa məlumat bloqun ötürülür.



Şəkil: Modelin arxitekturası

Lakin bütün istəklər yalnız buəməliyyatlarından ibarətdir, əksər hallarda istifadəçilərdən və ya hesablama sistemindən alınan məlumatlar üzrə hesablamalar kimi əlavə mantıksal əməliyyatlar var. Bu səbəbdən verilənlər bloku ilə birlikdə həyata keçirilən mantıksal əməliyyatlardan məsul olan alqoritm blokunu əlavə edir.

Nəhayət, yuxarıda təklif olunan hesablama modelindən əlavə blokumuz var. Əvvəlki bəndlərdə dəqiq nəticəyə nail olmaq üçün müstəqil və ya birlikdə işləyən məlumat və alqoritm bloklarını göstərdik. Amma tələb edilə biləcək əməliyyatların ölçüsü bu iki ilə məhdudlaşmır. Bununla yanaşı, digər məlumat sistemləri və hesablama sistemləri arasında məlumatların göndərilməsindən və ya alınmasından ibarət olan bəzi əməliyyatlar var, məsələn, bank əməliyyatları əsasən bu cür əməliyyatlardan ibarətdir. Hal-hazırda, xidmətə yönəldilən proqramın məşhur olduğu üçün, bu cür əməliyyatlar daha çox baş verir. Bu cür əməliyyat növlərini nəzərə alaraq, onların modelləşdirilməsi zamanı onların ardıcıllığı da çox vacibdir. Fərqli mümkün sorğu növlərinə əsaslanan ardıcıllıqla təşkil edilən əhəmiyyətli permütasyonlar aşağıda verilmişdir.

Nəticə

Bu məqalə performansını anonimləşdirilmiş verilənlər bazası ilə qiymətləndirən fırıldaqçılıq aşkarlama modelini təklif etdi və təklif olunan model bu xüsusiyyətlərdən asılıdır. Təklif olunan modelin ikinci xüsusiyyəti sinif balanssızlığını idarə etmək bacarığıdır. Bu fırıldaqçılıq və qanuni əməliyyatlar üçün iki ayrı nümunə verilənlər bazası yaratmaqla modelə daxil edilmişdir. Həm müştəri, həm də səhv davranışlar uzun müddət ərzində tədricən dəyişir. Bu, fırıldaqçılıq aşkarlama modelinin performansını azalda bilər. Buna görə də fırıldaqçılıq aşkarlama modeli bu davranış dəyişikliyinə uyğun olmalıdır. Bu davranış dəyişiklikləri, fırıldaqçılıq və qanuni nümunə veritabanlarını yeniləməklə təklif olunan modelə daxil edilə bilər.

ƏDƏBİYYAT

1. Məqalə: Bhattacharyya, S., Jha, S., Kurian Tharakunnel, J. Westland, C., Data mining for credit card fraud: A comparative study, Decision Support Systems, Vol-50, 602–613, (2011). **2**. **Məqalə**: Richard J. Bolton and David J. Hand, Peer Group Analysis – Local Anomaly Detection in Longitudinal Data.http: // citeseerx. ist.psu. edu/ viewdoc/download?doi=10.1.1.25.4115&rep=rep1&type=pdf, (2007). **3. Məqalə**: Deshpande Poonam. 'Fraud detection in Debit card transactions' presented in the International conference on Cost Benefit Analysis at Thakur college of Science and Commerce, Mumbai, India, 2015,

Применение технологий данных горения для обнаружения мошенничества в операциях карты

Н.Ф.Алиев

.Хотя термин FRAUD имеет другое определение и несколько полей для назначения, основной сбой из-за мошенничества связан с транзакцией «Card Not Present», такой как онлайн-покупка, почтовые транзакции, телефонные транзакции и т. Д. Убытки от мошенничества с карты в миллиарды долларов и на подъеме. Мошенники всегда находят новые способы совершения мошенничества, и они знают, как обойти систему. В большинстве случаев обнаружение мошенничества происходит после того, как мошенничество уже совершено, и многие из мошенников остаются не обнаруженными.. Поэтому методы обнаружения мошенничества с кредитными картами требуют постоянных инноваций, и все финансовые учреждения должны иметь некоторые методы или методы обнаружения мошенничества для решения такого сценария. Data Mining - это в основном инструмент для обнаружения шаблона, обнаружения выбросов или аномалий. Он хорошо работает для обнаружения различных видов мошенничества. В этом документе анализируются различные методы обнаружения мошенничества на основе интеллектуального анализа данных, такие как нейронная сеть, поддерживающая векторные машины, ближайший сосед К, искусственная иммунная система, анализ групп сверстников и т. Д. Мы также предлагаем предложения по новой методике, которая может быть реализована и которые поймут суть существующих технологий и могут объединить некоторые из них, чтобы обеспечить отличный инструмент обнаружения мошенничества.

Ключевые слова: разработка программного обеспечения, жизненный цикл разработки программного обеспечения, архитектура контроллера-вида-модели, сбор данных

Applications of data mining techniques for fraud detection in card transactions

N.F.Aliyev

While the term FRAUD has a different definition and several fields for appointing, the main failure due to fraud is related to the transaction "Card Not Present", such as online purchase, mail transactions, telephone transactions, etc. Fraud losses from the card is in billions of dollars and on the rise. Scammers always find new ways to commit fraud, and they know how to get around the system. In most cases, fraud detection occurs after fraud has already been committed, and many of the scammers remain undetected. Therefore, methods for detecting credit card fraud require constant innovation, and all financial institutions must have some fraudulent detection methods or methods to deal with such a scenario. Data Mining is basically a tool for detecting a pattern, detecting emissions or anomalies. It works well for detecting various types of fraud. This paper analyzes various methods for detecting fraud based on data mining, such as a neural network supporting vector machines, K-nearest neighbor, artificial immune system, peer group analysis, etc. We also offer suggestions for a new technique that can be implemented and that will grasp the essence of existing technologies and can combine some of them to provide an excellent fraud detection tool.

Key words: Software engineering, software development life cycle, model-view-controller architecture.

e-mail- nfaliyev@gmail.com

